【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成18年12月14日(2006.12.14)

【公開番号】特開2005-286959(P2005-286959A)
【公開日】平成17年10月13日(2005.10.13)
【年通号数】公開・登録公報2005-040
【出願番号】特願2004-102039(P2004-102039)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
Ｇ０６Ｆ　21/24　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ｂ
Ｇ０６Ｆ　12/14　５３０Ｃ
Ｇ０６Ｆ　12/14　５３０Ｐ
Ｇ０６Ｆ　12/14　５４０Ｃ
Ｈ０４Ｌ　9/00　６０１Ｅ

【手続補正書】
【提出日】平成18年10月30日(2006.10.30)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
階層木構成に基づくブロードキャストエンクリプション方式により特定選択機器のみの復号を可能とした暗号文の提供処理に適用する階層木を生成する情報処理方法であり、
階層木を適用したＳＤ（Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ）方式に基づいて設定するサブセット各々に対応するラベル（ＬＡＢＥＬ）中、選択された一部の特別サブセットに対応するラベルの値を演算処理により算出可能な値として設定した中間ラベル（ＩＬ）であり、少なくとも１つの中間ラベルの値に基づく落とし戸つき一方向性置換Ｆの適用により他の中間ラベルの値を算出可能な値を持つ中間ラベルを生成する中間ラベル生成ステップと、
前記中間ラベルに基づく演算処理により、前記特別サブセット対応のラベルを生成し、さらに該生成ラベルに基づく演算により特別サブセット非対応のラベルを生成するラベル生成ステップと、
前記階層木の末端ノード対応の受信機に対する提供ラベルを決定するステップであり、
前記特別サブセットに対応しない特別サブセット非対応ラベルと、
演算処理によって前記特別サブセットに対応するラベルを算出可能とした中間ラベルと、
を受信機に対する提供ラベルとして決定する提供ラベル決定ステップと、
を有することを特徴とする情報処理方法。
【請求項２】
階層木構成に基づくブロードキャストエンクリプション方式であるＳＤ（Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ）方式に基づいて設定するサブセット各々に対応するサブセットキーによって暗号化された暗号文の復号処理を実行する復号処理方法であり、
前記暗号文から、自己の保持するラベル、または自己の保持する中間ラベルから算出可能なラベルに基づく擬似乱数生成処理によって導出可能なサブセットキーを適用して生成

した暗号文を選択する暗号文選択ステップと、
暗号文の適用サブセットキーが、保持ラベルに基づく擬似乱数生成処理によって導出可能なサブセットキーでない場合に、保持中間ラベルに対する演算処理を実行して特別サブセット対応のラベルを算出するラベル算出ステップと、
保持ラベルまたは算出ラベルに基づく擬似乱数生成処理によってサブセットキーを生成するステップと、
生成サブセットキーを適用して暗号文の復号処理を実行する復号ステップと、
を有することを特徴とする復号処理方法。
【請求項３】
階層木構成に基づくブロードキャストエンクリプション方式により特定選択機器のみの復号を可能とした暗号文の生成処理を実行する情報処理方法であり、
階層木を適用したＳＤ（Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ）方式に基づいて設定するサブセット各々に対応するサブセットキーを選択的に適用して暗号化処理を実行して暗号文を生成する暗号文生成ステップを有し、
暗号文生成ステップにおいて適用するサブセットキーは、
サブセット各々に対応するラベル（ＬＡＢＥＬ）から算出可能なサブセットキーであり、選択された一部の特別サブセットに対応するラベルの値が、中間ラベル（ＩＬ）に基づく演算処理により算出可能であり、前記中間ラベルは、少なくとも１つの中間ラベルの値に基づく落とし戸つき一方向性置換Ｆの適用により他の中間ラベルの値を算出可能な設定であることを特徴とする情報処理方法。
【請求項４】
階層木構成に基づくブロードキャストエンクリプション方式により特定選択機器のみの復号を可能とした暗号文の提供処理に適用する階層木を生成する情報処理装置であり、
階層木を適用したＳＤ（Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ）方式に基づいて設定するサブセット各々に対応するラベル（ＬＡＢＥＬ）中、選択された一部の特別サブセットに対応するラベルの値を演算処理により算出可能な値として設定した中間ラベル（ＩＬ）であり、少なくとも１つの中間ラベルの値に基づく落とし戸つき一方向性置換Ｆの適用により他の中間ラベルの値を算出可能な値を持つ中間ラベルを生成する中間ラベル生成手段と、
前記中間ラベルに基づく演算処理により、前記特別サブセット対応のラベルを生成し、さらに該生成ラベルに基づく演算により特別サブセット非対応のラベルを生成するラベル生成手段と、
前記階層木の末端ノード対応の受信機に対する提供ラベルを決定する提供ラベル決定手段であり、
前記特別サブセットに対応しない特別サブセット非対応ラベルと、
演算処理によって前記特別サブセットに対応するラベルを算出可能とした中間ラベルと、
を受信機に対する提供ラベルとして決定する提供ラベル決定手段と、
を有することを特徴とする情報処理装置。
【請求項５】
前記情報処理装置は、さらに、
前記ラベル生成手段において生成したサブセット対応の各ラベルから導出されるサブセットキーを選択的に適用して暗号化処理を実行して暗号文を生成し、前記受信機に提供する暗号文生成手段を有することを特徴とする請求項４に記載の情報処理装置。
【請求項６】
前記ラベル生成手段は、
中間ラベルに対するハッシュ算出処理により、特別サブセットに対応するラベルの値を算出する構成であることを特徴とする請求項４に記載の情報処理装置。
【請求項７】
前記ラベル生成手段は、

特別サブセットに対応するラベルの値に対する擬似乱数生成処理により、他のラベルを生成する構成であることを特徴とする請求項４に記載の情報処理装置。

【請求項８】

前記中間ラベル生成手段は、

ノード数２Ｎ－１の階層木において、値$x_1 \in Z^*_M$をランダムに選択し、ｉをカウンタとして、ｉ＝２～２Ｎ－１までｉを１つずつ増加させながら、落とし戸つき一方向性置換Ｆの逆置換F^{-1}を適用した演算式である下記式、

【数３】

$$x_i = (x_{\lfloor i/2 \rfloor} + i)^d \bmod M$$

ただし、$\lfloor i \rfloor$は、ｉ以下の最大の整数を示す

または、下記式、

【数４】

$$x_i = (x_{\lfloor i/2 \rfloor} + h(i))^d \bmod M$$

ただし、$\lfloor i \rfloor$は、ｉ以下の最大の整数を示す

ただし、Ｍ、ｄは、暗号パラメータとしての法Ｍおよび秘密指数ｄ、

上記式のいずれかを適用して、ノード数２Ｎ－１の階層木におけるノード対応値x_1～x_{2N-1}を算出し、これを、特別サブセット対応ラベルを算出可能な中間ラベル（ＩＬ）の値として設定する構成であることを特徴とする請求項４に記載の情報処理装置。

【請求項９】

前記中間ラベル生成手段において選択する特別サブセットは、

階層木において、ノードｉを頂点とする部分木からノードｉより下層のノードｊを頂点とする部分木を除く集合として定義されたサブセット$S_{i,j}$中、ノードｉおよびノードｊが階層木において直結された親子関係にある第１特別サブセットと、

階層木のすべてのリーフを含むルートを頂点とする全体木の集合として定義されたサブセット$S_{1,\phi}$である第２特別サブセットと、

の少なくともいずれかであることを特徴とする請求項４に記載の情報処理装置。

【請求項１０】

前記提供ラベル決定手段は、

前記階層木の末端ノード対応の受信機に提供する１つの中間ラベルを前記第１特別サブセットを構成するサブセット$S_{i,j}$中、最下層のサブセットに対応する中間ラベルとすることを特徴とする請求項４に記載の情報処理装置。

【請求項１１】

前記中間ラベル生成手段は、

階層木中に設定した１つの特別レベルによって分離したレイヤ別のサブセット管理構成を持つベーシックＬＳＤ（Ｂａｓｉｃ　Ｌａｙｅｒｅｄ　Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ）方式に従って設定するサブセット各々に対応するラベル（ＬＡＢＥＬ）中、選択

された一部の特別サブセットに対応するラベルを、該特別サブセット対応の中間ラベル（ＩＬ）から算出可能な値として設定する手段であることを特徴とする請求項４乃至１０いずれかに記載の情報処理装置。

【請求項１２】

前記中間ラベル生成手段は、

階層木中に設定した複数の特別レベルによって分離したレイヤ別のサブセット管理構成を持つ一般化ＬＳＤ（Ｇｅｎｅｒａｌ Ｌａｙｅｒｅｄ Ｓｕｂｓｅｔ Ｄｉｆｆｅｒｅｎｃｅ）方式に従って設定するサブセット各々に対応するラベル（ＬＡＢＥＬ）中、選択された一部の特別サブセットに対応するラベルを、該特別サブセット対応の中間ラベル（ＩＬ）から算出可能な値として設定する手段であることを特徴とする請求項４乃至１０いずれかに記載の情報処理装置。

【請求項１３】

階層木構成に基づくブロードキャストエンクリプション方式であるＳＤ（Ｓｕｂｓｅｔ Ｄｉｆｆｅｒｅｎｃｅ）方式に基づいて設定するサブセット各々に対応するサブセットキーによって暗号化された暗号文の復号処理を実行する情報処理装置であり、

前記暗号文から、自己の保持するラベル、または自己の保持する中間ラベルから算出可能なラベルに基づく擬似乱数生成処理によって導出可能なサブセットキーを適用して生成した暗号文を選択する暗号文選択手段と、

暗号文の適用サブセットキーが、保持ラベルに基づく擬似乱数生成処理によって導出可能なサブセットキーでない場合に、保持中間ラベルに対する演算処理を実行して特別サブセット対応のラベルを算出するラベル算出手段と、

保持ラベルまたは算出ラベルに基づく擬似乱数生成処理によってサブセットキーを生成するサブセットキー生成手段と、

生成サブセットキーを適用して暗号文の復号処理を実行する復号手段と、

を有することを特徴とする情報処理装置。

【請求項１４】

前記ラベル算出手段は、

保持中間ラベルに対する落とし戸つき一方向性置換Ｆの実行より他の中間ラベルを算出する構成であることを特徴とする請求項１３に記載の情報処理装置。

【請求項１５】

前記ラベル算出手段は、

保持中間ラベル、または、保持中間ラベルに対する落とし戸つき一方向性置換Ｆの実行より算出した他の中間ラベルに対するハッシュ演算によるラベル算出を実行する構成であることを特徴とする請求項１３に記載の情報処理装置。

【請求項１６】

前記ラベル算出手段は、

暗号文の適用サブセットキーが、

階層木においてノードｉを頂点とする部分木からノードｉより下層のノードｊを頂点とする部分木を除く集合として定義されたサブセット$S_{i,j}$中、ノードｉおよびノードｊが階層木において直結された親子関係にある第１特別サブセット、または、階層木のすべてのリーフを含むルートを頂点とする全体木の集合として定義されたサブセット$S_{1,\phi}$である第２特別サブセット、

のいずれかの特別サブセット対応のラベルに基づく擬似乱数生成処理により算出可能なサブセットキーであり、前記特別サブセット対応のラベルを保持していない場合に、保持している中間ラベルに対する演算処理により前記特別サブセット対応のラベルを算出する構成であることを特徴とする請求項１３に記載の情報処理装置。

【請求項１７】

前記ラベル算出手段は、

前記階層木において、復号処理を実行する受信機の設定ノードからルートに至るパス上のノードを包含する特別サブセットに対応するラベルの算出を保持中間ラベルに対する演

算処理により算出する構成であることを特徴とする請求項１３に記載の情報処理装置。
【請求項１８】
階層木構成に基づくブロードキャストエンクリプション方式により特定選択機器のみの復号を可能とした暗号文の生成処理を実行する情報処理装置であり、
階層木を適用したＳＤ（Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ）方式に基づいて設定するサブセット各々に対応するサブセットキーを選択的に適用して暗号化処理を実行して暗号文を生成する暗号文生成手段を有し、
暗号文生成手段において適用するサブセットキーは、
サブセット各々に対応するラベル（ＬＡＢＥＬ）から算出可能なサブセットキーであり、選択された一部の特別サブセットに対応するラベルの値が、中間ラベル（ＩＬ）に基づく演算処理により算出可能であり、前記中間ラベルは、少なくとも１つの中間ラベルの値に基づく落とし戸つき一方向性置換Ｆの適用により他の中間ラベルの値を算出可能な設定であることを特徴とする情報処理装置。
【請求項１９】
前記情報処理装置は、さらに、
サブセットキーを生成するサブセットキー生成手段を有し、
前記サブセットキー生成手段は、
サブセット各々に対応するラベル（ＬＡＢＥＬ）に基づく擬似乱数生成処理によりサブセットキーを生成する構成であることを特徴とする請求項１８に記載の情報処理装置。
【請求項２０】
前記情報処理装置は、さらに、
サブセットキーを生成するサブセットキー生成手段を有し、
前記サブセットキー生成手段は、
値$x_1 \in Z^*_M$と、暗号パラメータとしての法Ｍおよび秘密指数ｄとを適用した落とし戸つき一方向性置換Ｆの逆置換F^{-1}を適用した演算式に基づいて、前記特別サブセットに対応する中間ラベルを生成し、前記中間ラベルに基づく演算処理により、前記特別サブセット対応のラベルを生成し、さらに該生成ラベルに基づく演算により特別サブセット非対応のラベルを生成し、生成ラベルに基づく演算処理によりサブセットキーを算出する構成であることを特徴とする請求項１８に記載の情報処理装置。
【請求項２１】
前記特別サブセットは、
階層木において、ノードｉを頂点とする部分木からノードｉより下層のノードｊを頂点とする部分木を除く集合として定義されたサブセット$S_{i,j}$中、ノードｉおよびノードｊが階層木において直結された親子関係にある第１特別サブセットと、
階層木のすべてのリーフを含むルートを頂点とする全体木の集合として定義されたサブセット$S_{1,\phi}$である第２特別サブセットと、
の少なくともいずれかであることを特徴とする請求項１８に記載の情報処理装置。
【請求項２２】
前記サブセットは、階層木中に設定した１つの特別レベルによって分離したレイヤ別のサブセット管理構成を持つベーシックＬＳＤ（Ｂａｓｉｃ　Ｌａｙｅｒｅｄ　Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ）方式に従って設定するサブセットであることを特徴とする請求項１８に記載の情報処理装置。
【請求項２３】
前記サブセットは、階層木中に設定した複数の特別レベルによって分離したレイヤ別のサブセット管理構成を持つ一般化ＬＳＤ（Ｇｅｎｅｒａｌ　Ｌａｙｅｒｅｄ　Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ）方式に従って設定するサブセットであることを特徴とする請求項１８に記載の情報処理装置。
【請求項２４】
階層木構成に基づくブロードキャストエンクリプション方式により特定選択機器のみの復号を可能とした暗号文の提供処理に適用する階層木を生成するコンピュータ・プログラ

ムであり、
階層木を適用したＳＤ（Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ）方式に基づいて設定するサブセット各々に対応するラベル（ＬＡＢＥＬ）中、選択された一部の特別サブセットに対応するラベルの値を演算処理により算出可能な値として設定した中間ラベル（ＩＬ）であり、少なくとも１つの中間ラベルの値に基づく落とし戸つき一方向性置換Ｆの適用により他の中間ラベルの値を算出可能な値を持つ中間ラベルを生成する中間ラベル生成ステップと、
前記中間ラベルに基づく演算処理により、前記特別サブセット対応のラベルを生成し、さらに該生成ラベルに基づく演算により特別サブセット非対応のラベルを生成するラベル生成ステップと、
前記階層木の末端ノード対応の受信機に対する提供ラベルを決定するステップであり、
前記特別サブセットに対応しない特別サブセット非対応ラベルと、
演算処理によって前記特別サブセットに対応するラベルを算出可能とした中間ラベルと、
を受信機に対する提供ラベルとして決定する提供ラベル決定ステップと、
を有することを特徴とするコンピュータ・プログラム。
【請求項２５】
階層木構成に基づくブロードキャストエンクリプション方式であるＳＤ（Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ）方式に基づいて設定するサブセット各々に対応するサブセットキーによって暗号化された暗号文の復号処理を実行するコンピュータ・プログラムであり、
前記暗号文から、自己の保持するラベル、または自己の保持する中間ラベルから算出可能なラベルに基づく擬似乱数生成処理によって導出可能なサブセットキーを適用して生成した暗号文を選択する暗号文選択ステップと、
暗号文の適用サブセットキーが、保持ラベルに基づく擬似乱数生成処理によって導出可能なサブセットキーでない場合に、保持中間ラベルに対する演算処理を実行して特別サブセット対応のラベルを算出するラベル算出ステップと、
保持ラベルまたは算出ラベルに基づく擬似乱数生成処理によってサブセットキーを生成するステップと、
生成サブセットキーを適用して暗号文の復号処理を実行する復号ステップと、
を有することを特徴とするコンピュータ・プログラム。
【請求項２６】
階層木構成に基づくブロードキャストエンクリプション方式により特定選択機器のみの復号を可能とした暗号文の生成処理を実行するコンピュータ・プログラムであり、
階層木を適用したＳＤ（Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ）方式に基づいて設定するサブセット各々に対応するサブセットキーを選択的に適用して暗号化処理を実行して暗号文を生成する暗号文生成ステップを有し、
暗号文生成ステップにおいて適用するサブセットキーは、
サブセット各々に対応するラベル（ＬＡＢＥＬ）から算出可能なサブセットキーであり、選択された一部の特別サブセットに対応するラベルの値が、中間ラベル（ＩＬ）に基づく演算処理により算出可能であり、前記中間ラベルは、少なくとも１つの中間ラベルの値に基づく落とし戸つき一方向性置換Ｆの適用により他の中間ラベルの値を算出可能な設定であることを特徴とするコンピュータ・プログラム。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００２２
【補正方法】削除
【補正の内容】
【手続補正３】
【補正対象書類名】明細書

【補正対象項目名】００２３
【補正方法】削除
【補正の内容】
【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】００２４
【補正方法】削除
【補正の内容】
【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】００２５
【補正方法】削除
【補正の内容】
【手続補正６】
【補正対象書類名】明細書
【補正対象項目名】００２６
【補正方法】削除
【補正の内容】
【手続補正７】
【補正対象書類名】明細書
【補正対象項目名】００２７
【補正方法】削除
【補正の内容】
【手続補正８】
【補正対象書類名】明細書
【補正対象項目名】００２８
【補正方法】削除
【補正の内容】
【手続補正９】
【補正対象書類名】明細書
【補正対象項目名】００２９
【補正方法】削除
【補正の内容】
【手続補正１０】
【補正対象書類名】明細書
【補正対象項目名】００３１
【補正方法】削除
【補正の内容】
【手続補正１１】
【補正対象書類名】明細書
【補正対象項目名】００３２
【補正方法】削除
【補正の内容】
【手続補正１２】
【補正対象書類名】明細書
【補正対象項目名】００３３
【補正方法】削除
【補正の内容】
【手続補正１３】
【補正対象書類名】明細書

【補正対象項目名】００３４
【補正方法】削除
【補正の内容】
【手続補正１４】
【補正対象書類名】明細書
【補正対象項目名】００３６
【補正方法】削除
【補正の内容】
【手続補正１５】
【補正対象書類名】明細書
【補正対象項目名】００３７
【補正方法】削除
【補正の内容】
【手続補正１６】
【補正対象書類名】明細書
【補正対象項目名】００３８
【補正方法】削除
【補正の内容】
【手続補正１７】
【補正対象書類名】明細書
【補正対象項目名】００３９
【補正方法】削除
【補正の内容】
【手続補正１８】
【補正対象書類名】明細書
【補正対象項目名】００４０
【補正方法】削除
【補正の内容】